

Data Loss Prevention Policy 1/6/2018

Policy Statement

Spectrum Analysis' exist for the purpose of conducting legitimate business. Spectrum Analysis is bound by state and federal law to protect certain information that is transmitted using Spectrum Analysis' systems, hardware, and networks. Pursuant to these objectives, Spectrum Analysis has a duty to actively prevent the loss of Protected Information.

It is the policy of the Spectrum Analysis to engage in sustained and substantial efforts to provide for the confidentiality and integrity of Protected Information; to promptly discover and remedy any Security Breach or misuse of Information Technology Resources; and to expeditiously take those measures needed to reduce the probability of a Security Breach or a misuse of Information Technology Resources. This Policy is intended to further and not replace, in whole or in part, approved Policies dealing with the collection, storage, maintenance, transmission and use of Data.

Policy Manager

Peter Buckingham – Managing Director – Spectrum Analysis Australia Pty Ltd

Purpose/Reason for the Policy

This Policy establishes the principles by which Spectrum Analysis will identify, protect and respond to the unauthorized disclosure of Protected Information by electronic means. The specific purposes of this Policy are to:

- (a) further enable and affirm the particular responsibilities of the Chief Data Scientist for monitoring and reporting compliance with Policy.
- (b) authorize Spectrum Analysis to take reasonable measures to secure Protected Information by using, among other techniques and methods, Data Loss Prevention (DLP) software and equipment to monitor, identify and block the unauthorized disclosure of Protected Information;
- (c) prescribe mechanisms that help to identify and address areas of high risk for the unauthorized release of Protected Information and the misuse of Data, applications, Spectrum Analysis Network and Computers.

Personnel Affected by the Policy

This Policy is applicable to all members of Spectrum Analysis staff and contractors who may have access to Customer Data regardless of the electronic medium in which such Data are stored and regardless of where such Data may be located.

Procedures Related to the Policy

1.0 DEFINITIONS

The terms listed below have the meanings ascribed next to each:

- (a) "CDS" – means Spectrum Analysis's Chief Data Scientist or any successor position.
- (b) "Computer" – means any computer that is owned, leased or rented by Spectrum Analysis whether such computer is located on or off Spectrum Analysis premises.
- (d) "Network" – means any part of Spectrum Analysis's Data, voice or video network physically located on any Spectrum Analysis owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such network assigned any routable and non- routable IP addresses and applies to Spectrum Analysis's wireless network.
- (e) "Data" means electronic information whether stored digitally or in text, voice, code or visual representation or in any other electronic medium.
- (f) "Data-At- Rest"- means stored or archived Data and includes, but is not limited to, Data stored on Information Technology Resources.
- (g) "Data-In-Motion" -- means Data that is traversing Spectrum Analysis Network or otherwise being transferred electronically and includes, but is not limited to, email, instant messages, ftp, and web traffic utilizing Information Technology Resources.
- (h) "Data-in-Use"- means Data that is being manipulated by a user, and includes, but is not limited to, transferring Data to a USB drive or copying, altering and/or pasting Data.
- (i) "IT"— Spectrum Analysis's Information Technology.
- (j) "Information Technology Resources" – Spectrum Analysis Network Computers and computer components, electronic storage devices, wiring, and electronic transmission devices owned, leased, rented or operated by Spectrum Analysis and all owned or licensed software.
- (k) "Protected Information"- Protected Information is a single term that includes all of the following: Confidential Information, Personal Information, and Proprietary Data of Spectrum Analysis and Customer data.

(l) "Security Breach"- the unauthorized disclosure of Protected Information. Spectrum Analysis will classify such Breaches by various levels of severity that will, in turn, specify the types of responses appropriate to the level of severity the breach is assigned.

2.0 SECURITY REVIEWS

2.1 Scope. Based upon a determination made by the CDS in accordance with the provisions of Section 2.2, Spectrum Analysis may:

- (a) access and examine Computers and other Information Technology Resources and all Data (whether Data-In-Motion, Data-At-Rest, or Data-In-Use) utilizing Information Technology Resources in any manner whatsoever;
- (b) monitor Spectrum Analysis Network activities of individual computer users of Information Technology Resources;
- (c) conduct a forensic analysis of Information Technology Resources, and the use and usage of such Resources.

2.2 Determinations. The Chief Data Scientist (CDS) may exercise the rights of Spectrum Analysis and take one or more of the actions described in Section 2.1 if the CDS reasonably determines that such action is necessary or appropriate to –

- (a) protect the integrity or security of Protected Information or Information Technology Resources;
- (b) protect Spectrum Analysis from incurring liability;
- (c) reduce the risk of the deliberate or unwitting disclosure of Protected Information or security features of Spectrum Analysis's Network that are not publically known;
- (d) investigate unusual or excessive activity typically associated with illegal activity or activity that may be in violation of acceptable use of Information Technology Resources or data;

3.0 PROBABLE VIOLATIONS

3.1 Confirmation. In the event that IT personnel identify or are made aware of a probable violation of a policy through the misuse of an Information Technology Resource, the incident shall be recorded in secure Information Security records system and a notification and description of the incident shall be sent to the Chief Data Scientist for further review and analysis. If the Chief Data Scientist concurs that a probable violation has occurred or is likely to occur, such Officer shall promptly notify the Managing Director of Spectrum Analysis.

3.2 Notifications. Upon receiving notification pursuant to Section 3.1, the CDS shall then determine what additional notifications, if any, should be made, except that in all cases of suspected criminal activity the Police shall be promptly notified.

4.0 CONFIDENTIALITY

4.1 Confidentiality Agreements. IT personnel having knowledge of, or access to, the equipment, software, data or methods shall be required to sign a Confidentiality Agreement as a condition of employment and continued employment by Spectrum Analysis. Such Agreement shall be in a form and substance as mutually agreed upon by the Managing Director of Spectrum Analysis. The Agreement will be maintained and reviewed annually.

5.0 POLICY COMPLIANCE AND MAINTENANCE

5.1 Sanctions. Employees are expected to cooperate with the IT Office with respect to the implementation of this Policy. Any person who knowingly attempts to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by Spectrum Analysis for the purpose of implementing this Policy shall be subject to appropriate disciplinary and remedial actions, up to and including termination of employment, and/or legal action.

6.0 DISTRIBUTION AND TRAINING

The CDS of Spectrum Analysis shall ensure that this Policy is distributed to all employees. The CDS shall be responsible for devising and implementing such employee training programs and information as he believes necessary and appropriate to effectively implement this Policy.

7.0 OPERATING PROCEDURES

The CDS shall adopt such operating procedures to implement this Policy as maybe appropriate, provided that, such operating procedures are not in conflict with any provision of this Policy and are made readily available to all at Spectrum Analysis.